A system for providing secure access to secure information

ABSTRACT

A method and apparatus for utilizing a random token, preferably a non-repetitive "dumb token", for secure access by authorized users to sensitive information, specifically as a part of a system where the security algorithm and / or the password cannot be modified and / or updated during consecutive data exchange sessions. The token is generated by the Token Generator (TG) and should be presented in machine readable form to a Token Processor (TP). The TP uses the token in order to generate a secure key and an encoding sequence. The key, which may be time varying, should be sent back to the TG where it is used to generate a decoding sequence. The TP encodes the secure information using the encoding sequence and sends it to the TG, which decodes the secure information using the decoding sequence.

CROSS-REFERENCE TO RELATED APPLICATIONS

For example, parent U.S. Pat. No. 5,023,908, discloses a secure communication system, wherein the end device in the possession of the individual is utilized to generate a unique, time varying and non-predictable code. The said non-predictable code is muxed with the personal identification number (PIN) and sent to the central verification computer, which verifies the validity of the PIN. This technique provides the user with high level of security in data transmission, but cannot guarantee required level of security in systems which don't have an ability to modify its PIN over time and / or adjust the technique used for muxing the said varying non-predictable code with the PIN. The fact that neither copyright protection titles, nor personal identification cards can rely on their PINs to be changed over time, by virtue of being used by not only highly trained

professionals, but by the general population as well, requires new techniques to be developed in order to maintain desired level of security.

The obvious problem of the method discussed in U.S. Pat. No. 5,023,908 is linked to the fact that a "challenge" code is recommended for use in order to generate a non-predictable code, which in turn starts the sequence of events leading to successful secure data communication. The fact that the PIN (a fixed value) which has to be recognized by many (an infinite number) of end devices contrary to the central verification computer (as described in U.S. Pat. No. 5,023,908), make the data transmission vulnerable. A scenario when a set of quasi "challenge" codes is sent to the end device can be imagined. Suggested in U.S. Pat. No. 5,023,908 method of utilizing fixed algorithm of generating non-predictable code based on a "challenge" code guarantees that not only PIN value, but the data as well will be eventually exposed.

Other known methods of secure communication of the data over a not secure data transmission line also require PIN exchange. This as we know is not acceptable for applications, where multiple clients have identical PINs those PINs cannot be modified over time and all end devices must recognize all PINs of all current and all future clients (even those which at the time of the system development did not exist).

A need therefore exists for an improved means of communicating secure data over the not-secure data link. Means which don't require a PIN or other user identification code and don't rely on a central verification system such that someone tapping the line over which the code is being sent will be unable to determine the secret identification synchronization sequence and gain access to the information.

CLAIMS

What is claimed is: